

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
Please do not report the images to the
Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-211306

(43)Date of publication of application : 03.08.2001

(51)Int.Cl.

H04N 1/32
H04L 9/14
H04L 12/46
H04L 12/28
H04L 12/66
H04N 1/00
H04N 1/44

(21)Application number : 2000-323980

(71)Applicant : CANON INC

(22)Date of filing : 24.10.2000

(72)Inventor : SATO EIICHI

(30)Priority

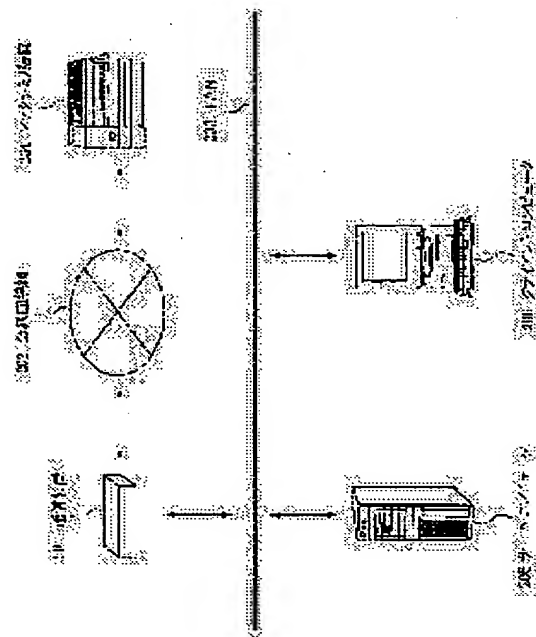
Priority number : 11325559 Priority date : 16.11.1999 Priority country : JP

(54) DEVICE AND METHOD FOR COMMUNICATION, AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a device and a method for communication, and a storage medium which can transfer a received confidential image to a prescribed destination while keeping its secrecy.

SOLUTION: The communication device which transfers received data from a 1st network to a 2nd network discriminates the transfer destination information and secrecy degree information of the received data and transfers the received data according to the decision results.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-211306

(P 2 0 0 1 - 2 1 1 3 0 6 A)

(43) 公開日 平成13年8月3日 (2001. 8. 3)

| (51) Int. Cl. ⁷ | 識別記号 | F I | テーマコード (参考) |
|------------------------------------|------|-----------|-------------|
| H04N 1/32 | | H04N 1/32 | Z |
| H04L 9/14 | | 1/00 | 104 Z |
| 12/46 | | 1/44 | |
| 12/28 | | H04L 9/00 | 641 |
| 12/66 | | 11/00 | 310 C |
| 審査請求 未請求 請求項の数20 O L (全16頁) 最終頁に続く | | | |

(21) 出願番号 特願2000-323980 (P 2000-323980)

(22) 出願日 平成12年10月24日 (2000. 10. 24)

(31) 優先権主張番号 特願平11-325559

(32) 優先日 平成11年11月16日 (1999. 11. 16)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 佐藤 栄一

東京都大田区下丸子3丁目30番2号キヤノ
ン株式会社内

(74) 代理人 100090538

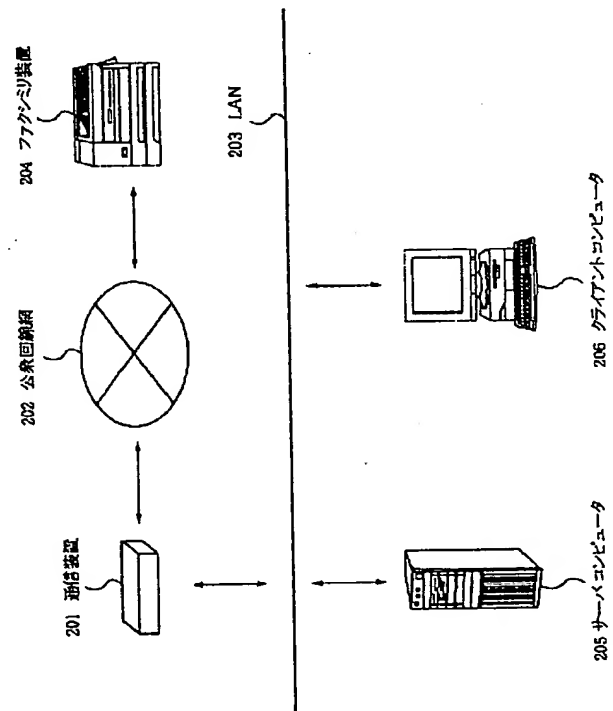
弁理士 西山 恵三 (外1名)

(54) 【発明の名称】 通信装置及び方法並びに記憶媒体

(57) 【要約】

【課題】 受信した親展画像をその機密性を維持したまま所定の宛先に転送することが可能な通信装置及び方法並びに記憶媒体を提供することを目的とする。

【解決手段】 第1のネットワークからの受信データを第2のネットワークへ転送する通信装置において、前記受信データの転送先情報と機密度情報をそれぞれ判別し、それらの判別結果に応じて、前記受信データの転送を実行する。



【特許請求の範囲】

【請求項 1】 第 1 のネットワークからの受信データを第 2 のネットワークへ転送する通信装置において、前記受信データの転送先情報を判別する第 1 の判別手段と、前記受信データの機密度情報を判別する第 2 の判別手段と、前記第 1 および第 2 の判別結果に応じて、前記受信データの転送を実行する制御手段を有することを特徴とする通信装置。

【請求項 2】 請求項 1 において、前記第 1 と第 2 の判別手段の少なくとも一方による判別に応じて、前記制御手段は前記受信データを暗号化して転送することを特徴とする通信装置。

【請求項 3】 請求項 1 において、前記機密度情報は、前記受信データが親展データであるかどうかを含むことを特徴とする通信装置。

【請求項 4】 請求項 1 において、前記第 1 と第 2 の判別手段の少なくとも一方による判別に応じて、前記制御手段は前記受信データを電子メールにより転送先に転送することを特徴とする通信装置。

【請求項 5】 請求項 1 において、前記第 1 と第 2 の判別手段の少なくとも一方による判別に応じて、前記制御手段は前記受信データを所定のメモリに記憶することを特徴とする通信装置。

【請求項 6】 請求項 1 において、前記転送先情報は、前記転送先に対応する暗号情報を具備しているかどうかを含むことを特徴とする通信装置。

【請求項 7】 請求項 1 において、前記転送先情報は、前記受信データの転送先への経路情報を含むことを特徴とする通信装置。

【請求項 8】 請求項 1 において、前記転送先情報は、前記転送先に対応する暗号情報が有効期限内にあるかどうかを含むことを特徴とする通信装置。

【請求項 9】 第 1 のネットワークからの受信データを第 2 のネットワークへ転送する通信方法において、前記受信データの転送先情報を判別する第 1 の判別工程と、前記受信データの機密度情報を判別する第 2 の判別工程と、前記第 1 および第 2 の判別結果に応じて、前記受信データの転送を実行する制御工程を有することを特徴とする通信方法。

【請求項 10】 第 1 のネットワークからの受信データを第 2 のネットワークへ転送する通信方法のプログラムを格納したコンピュータ読取可能な記憶媒体において、前記受信データの転送先情報を判別する第 1 の判別工程と、前記受信データの機密度情報を判別する第 2 の判別工程と、

前記第 1 および第 2 の判別結果に応じて、前記受信データの転送を実行する制御工程を実行するプログラムを格納したことを特徴とする記憶媒体。

【請求項 11】 第 1 のネットワークからの受信データを第 2 のネットワークへ転送する通信装置において、前記受信データの転送先に対応する暗号情報を有しているかどうか判断する判断手段と、前記判断に応じて、前記転送先に対応する暗号情報に基づいて暗号化した受信データを前記転送先に転送する、あるいは、前記受信データを所定のメモリに格納するように制御する制御手段を有することを特徴とする通信装置。

【請求項 12】 請求項 11 において、前記制御手段は前記受信データが所定のメモリに格納されたことを示すメッセージを前記転送先に送信することを特徴とする通信装置。

【請求項 13】 請求項 11 において、前記暗号情報は前記転送先から取得することを特徴とする通信装置。

【請求項 14】 請求項 11 において、前記制御手段は、前記受信データの機密度に応じて、前記暗号化を行うことを特徴とする通信装置。

【請求項 15】 請求項 11 において、前記制御手段は、前記転送先から暗号情報を取得すると、前記所定のメモリに格納された受信データを前記暗号情報により暗号化した後、前記転送先に転送することを特徴とする通信装置。

【請求項 16】 請求項 11 において、前記制御手段は前記転送先までの転送経路に応じて、前記暗号化を行うことを特徴とする通信装置。

【請求項 17】 請求項 11 において、前記暗号情報は有効期限を含むことを特徴とする通信装置。

【請求項 18】 請求項 17 において、前記暗号情報の有効期限は更新可能であることを特徴とする通信装置。

【請求項 19】 第 1 のネットワークからの受信データを第 2 のネットワークへ転送する通信方法において、前記受信データの転送先に対応する暗号情報を有しているかどうか判断する判断工程と、前記判断に応じて、前記転送先に対応する暗号情報に基づいて暗号化した受信データを前記転送先に転送する、あるいは、前記受信データを所定のメモリに格納するように制御する制御工程を有することを特徴とする通信方法。

【請求項 20】 第 1 のネットワークからの受信データを第 2 のネットワークへ転送する通信方法のプログラムを格納したコンピュータ読取可能な記憶媒体において、前記受信データの転送先に対応する暗号情報を有しているかどうか判断する判断工程と、前記判断に応じて、前記転送先に対応する暗号情報に基づいて暗号化した受信データを前記転送先に転送する、あるいは、前記受信データを所定のメモリに格納するように制御する制御工程を実行するプログラムを格納したこ

とを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、受信した機密データを転送するのに好適な通信装置に関する。

【0002】

【従来の技術】近年のインターネットの爆発的な普及により、従来は公衆回線を介してのみの通信を行っていたファクシミリ装置が、LAN (Local Area Network) 等のコンピュータネットワークにも接続されるようになってきた。

【0003】このような公衆回線網とLANに接続可能なマルチ回線対応のファクシミリ装置は、ファクシミリ装置から公衆回線網を経由して画像データを受信すると、該画像データをLAN経由でサーバコンピュータに転送する。

【0004】ユーザは、クライアントコンピュータによりサーバコンピュータにアクセスして画像データを取得する。取得した画像データは所定のビューソフトによりCRT上に表示して閲覧することができる。あるいは、クライアントコンピュータに接続されるプリンタにより、画像データを印刷して閲覧することもできる。

【0005】ところで、ファクシミリ通信には、親展機能と呼ばれる機能が存在する。これはファクシミリ装置が親展送信の指定とともに受信した画像をすぐに印刷せずにメモリに格納しておき、所定のパスワード入力により該メモリから印刷するものである。これにより、親展番号のパスワードを知るユーザにしか画像を閲覧することができないようにしたものである。

【0006】

【発明が解決しようとする課題】しかしながら、上記従来例のファクシミリ装置では、親展画像を転送するための構成が無い場合、親展文書の受取人であるユーザは、わざわざ当該ファクシミリ装置が設置してある場所まで出向いて、パスワードを入力することにより親展画像を印刷しなければならなかった。

【0007】

【課題を解決するための手段】本発明は、上記課題を解決するために、第1のネットワークからの受信データを第2のネットワークへ転送する通信装置において、前記受信データの転送先情報を判別する第1の判別手段と、前記受信データの機密度情報を判別する第2の判別手段と、前記第1および第2の判別結果に応じて、前記受信データの転送を実行する制御手段を有することを特徴とする通信装置を提供する。

【0008】また、本発明は、上記課題を解決するために、第1のネットワークからの受信データを第2のネットワークへ転送する通信装置において、前記受信データの転送先に対応する暗号情報を有しているかどうか判断する判断手段と、前記判断に応じて、前記転送先に対応

する暗号情報に基づいて暗号化した受信データを前記転送先に転送する、あるいは、前記受信データを所定のメモリに格納するように制御する制御手段を有することを特徴とする通信装置を提供する。

【0009】

【発明の実施の形態】以下、図面を参照しながら本発明に係る実施の形態を詳細に説明する。

【0010】図1は本発明の通信装置の構成を示したブロック図である。同図において101は装置全体の制御を司るCPU、102はCPU101が実行する制御プログラムが記憶されたROM、103はデータの一時保存領域となるRAMである。ここでRAMの一部は電池等によりバックアップされた不揮発性メモリになっており、本実施形態で必要な登録データや管理テーブル等、装置の電源がオフしても保持しておくべきデータが格納されている。尚、該不揮発性メモリはハードディスク装置等が代替してもよい。

【0011】104は外部回路とのデータの入出力を行うPIO、105はPIO104によって制御される操作パネル、106はデータを圧縮する圧縮回路、107はデータの伸張を行う伸張回路、108はデジタルデータを公衆回線網202に送出するために音声帯域のアナログ信号に変換するための変調回路、109は公衆回線網202から受信したアナログ信号をデジタル信号に復調する復調回路、110は変調回路108と復調回路109とからなるMODEM、111は本装置を公衆回線網202と接続するためのNCU、112は信号をLANへ送出するためのプロトコルに関する制御を司るLANコントローラ、113は信号レベルで本装置内の信号とLAN上の信号のマッチングを取るために利用されるLAN接続回路、114はCPU101が制御を行うために利用するCPUバスである。

【0012】また図2は本発明の通信装置201が接続されるネットワークシステムを示した図である。同図より、通信装置201は公衆回線網202とLAN203にそれぞれ接続されている。LAN203上には受信した画像データを保管する等の目的で利用されるサーバコンピュータ205、サーバコンピュータ205と情報交換が可能なクライアントコンピュータ206が接続されている。ここで、サーバコンピュータ205は、SMTPサーバ機能やPOPサーバ機能等の電子メールサーバ機能を備えており、通信装置201、クライアントコンピュータ206、並びにその他の不図示の端末との間で電子メールの交換が可能のように構成されている。ここで、通信装置201、および、クライアントコンピュータ206は、電子メールクライアント機能を備えていることは言うまでもない。

【0013】また、通信装置201は公衆回線網202を介してファクシミリ装置204とファクシミリ通信を実行する。

【0014】＜第1の実施形態＞第1の実施形態は、通信装置201が公衆回線網202から受信した画像データをサーバコンピュータ205に送信して所定の領域に格納する構成において、受信した画像データが親展画像か否かに基づいて画像データの暗号化処理を選択的に実行するものである。

【0015】すなわち、受信した画像データが親展画像である場合には、所定の方式により暗号化して格納することにより、特定のユーザしか閲覧できないようにする。これにより受信した親展画像の機密性を維持したまま転送することが可能となる。

【0016】以下、図3のフローチャートを用いて、本実施形態の通信装置201の動作を説明する。まず、通信装置201は電源投入後プログラムが開始（ステップS301）され、公衆回線網202の着信待ち状態（ステップS302）に移行する。着信の待機中に、ファクシミリ204からの発信があると、その呼が公衆回線網202を経由して通信装置201へ届き着信する。CPU101、NCU111によって当該着信を検知するとNCU111を用いて送信側と呼を確立する。

【0017】その後、ITU-T勧告T.30に準拠したフェーズBの処理へと移行し、通信能力情報の交換や通信回線の品質を調査するトレーニングを行う（これを事前交信として表す）。事前交信（ステップS303）では、前述のサブアドレス（ITU-T T.30におけるSUB信号による）や、親展画像の場合にはパスワード（ITU-T T.30におけるPWD信号による）、親展ボックス番号等の情報の通知が行われる。これらの情報は通信装置201内のRAM103へ一時的に保存される。

【0018】事前交信（ステップS303）が終了すると、画像データの受信（ステップS304）が実行される。ここでは、公衆回線網202を介して送られてきた画像信号が、NCU111から通信装置201内に取り込まれ、MODEM110の復調回路109を経て、伸張回路107によって元の画像データに戻された後、所定のデータ形式（圧縮データであってもよい）にしてCPU101によってRAM103に保存される。この受信動作は送信側から終了通知が届くまで繰り返して実行される（ステップS305）。

【0019】画像データの受信が終了すると、この画像が親展画像であるか否かを、前述したRAM103に保存された情報を読み出すことによって判断する（ステップS306）。尚、この判断では、上記のPWD信号を受信したか否かに基づいて判断してもよいし、NSS信号等の手順信号上で、親展機能を利用する旨の指定がされているか否かに基づいて判断してもよい。

【0020】画像データが親展画像であった場合は、CPU101によってRAM103へ保存した画像データを読み出した後、画像データの暗号化処理を行う（ステ

ップS307）。ここで、通信装置201は、サーバコンピュータ205に対応する暗号鍵で暗号化を行う。

【0021】そして、この暗号化された画像データをLANコントローラ112に送り、LAN接続回路113を介して、LAN203上へと送出し、サーバコンピュータ205へと転送する（ステップS308）。またCPU101は事前交信（ステップS303）で得たパスワードと親展ボックス番号を併せてサーバコンピュータ205へ送信し、通信装置201は処理を終了する（ステップS409）。

【0022】ステップS306において、画像データが親展画像でなかった場合は、暗号化の処理であるステップS307はパスされ、画像データを暗号化せずにサーバコンピュータ205へと転送（ステップS308）し、通信装置201は処理を終了する（ステップS309）。

【0023】ここで、上記ステップS308で転送された画像データを受信したサーバコンピュータ205は、該画像データを自身の記憶領域にファイルとして保存し、サブアドレスを元に画像データの受信通知を特定のユーザのクライアントコンピュータ206へ送信する。この通知手段は例えば電子メールによって行われる。

【0024】画像データが親展画像でない場合には、この通知を受け取ったユーザは、クライアントコンピュータ206を操作し、サーバコンピュータ205から自分宛に届いた画像データをダウンロードするなどして入手し、画像ビューアプリケーションを用いてクライアントコンピュータ206上に表示させたり、不図示のプリンタ装置を使って印刷させたりして画像データを可視情報として取得することが可能となる。

【0025】一方、画像データが親展画像であり、サーバコンピュータ205に保存された画像データが暗号化されている場合は、クライアントコンピュータ206がサーバコンピュータ205から画像データをダウンロードする際に親展ボックス番号に対応したパスワードをサーバコンピュータ205へ送信する必要がある。サーバコンピュータ205ではこのパスワードが正しい物であると判断した場合のみ、クライアントコンピュータ206へ復号化した画像データを送り、クライアントコンピュータ206を介して閲覧することが可能となる。

【0026】＜第2の実施形態＞第2の実施形態は、通信装置201が公衆回線網202から受信した画像データをサーバコンピュータ205に送信して所定の領域に格納する構成において、受信した画像データが親展画像である場合には、該格納を行わずに指定された転送先に電子メールにより転送するものである。

【0027】これにより、受信した画像データが親展画像である場合には、サーバコンピュータ205上のメモリに格納されることなく直接転送先に電子メール転送されるので、受信した親展画像の機密性を維持したまま転

送を実行することが可能となる。

【0028】以下、図4のフローチャートを用いて、本実施形態の通信装置201の動作を説明する。ここでステップS401～405の処理については、上記第1の実施形態のステップS301～305において説明しているので、ステップS406から説明する。

【0029】まず、ステップS405で受信した画像データが親展画像であるか否かを、前述したRAM103に保存された情報を読み出すことによって判別し（ステップS406）、親展画像の場合には、CPU101によってRAM103へ保存した画像データを読み出した後、CPU101は読み出した画像データをクライアントコンピュータ206によって展開が可能な画像フォーマット（JPEG、GIFなど）に変換する（ステップS407）。続いてCPU101はサブアドレスに基づいて転送先のクライアントコンピュータ206を特定し、電子メールを送信する（ステップS408）。その際、この電子メールに画像フォーマットに変換した画像データを添付して送ることにより、親展画像を特定のユーザに電子メールで届けることが実現する。画像フォーマットに変換した画像データを添付した電子メールの送信が終了すると、通信装置201は処理を終了する（ステップS409）。

【0030】ステップS406において、受信した画像データが親展画像でない場合は、画像データをサーバコンピュータ205へと転送（ステップS410）し、通信装置201は処理を終了する（ステップS409）。サーバコンピュータ205は受け取った画像データを自身の記憶領域にファイルとして保存し、サブアドレスを元に画像データの受信通知を特定のユーザのクライアントコンピュータ206へ送信する（ステップS411）。この通知手段は例えば電子メールによって行われる。この通知を受け取ったユーザは、クライアントコンピュータ206を操作し、サーバコンピュータ205から自分宛に届いた画像データをダウンロードするなどして入手し、画像ビューアアプリケーションを用いてクライアントコンピュータ206上に表示させたり、図示していないがプリンタ装置を使って印刷するなどして画像データを閲覧することが可能である。

【0031】＜第3の実施形態＞第3の実施形態として、受信した親展画像を電子メールで転送する際に、転送先の公開鍵を取得しているか否かに基づいて暗号化を選択的に実行する例を示す。

【0032】すなわち、通信装置201が、親展画像の転送先の公開鍵を取得している場合には、受信した画像データを該公開鍵により暗号化した電子メールにより転送する。通信装置201が、親展画像の転送先の公開鍵を取得していない場合には、該親展画像は転送せずに、通信装置201が管理するメモリボックスに格納しておき、転送先には、受信した親展画像をメモリボックスに

格納した旨を記載した電子メールのみを送信する。

【0033】ここで、公開鍵方式は、送信側の暗号化鍵と受信側の復号化鍵とが異なった暗号鍵であり、一方（公開鍵）を公開し、他方（秘密鍵）を秘密にするものである。自分の公開鍵で暗号化された親展画像を受信したユーザは、自分のみが所有する秘密鍵を用いて復号化して親展画像を閲覧すればよい。

【0034】これにより、親展画像が暗号化されずに、不用意にLAN上に流出してしまうのを防止し、親展画像の機密性を維持することが可能となる。

【0035】図6は、通信装置201が有するサブアドレスデータと転送先の電子メールアドレスとの対応を記憶した管理テーブルである。このテーブルには、サブアドレスデータ601に対する転送先の電子メールアドレスと親展ボックス番号とが対応づけられて記憶されている。

【0036】また、図7は、通信装置201の電子メールクライアント機能が有するアドレス帳のデータ構造をテーブルとして示した図である。同図より、宛先ごとに宛先名701、電子メールアドレス702、該宛先の公開鍵を所有しているか否かの情報703とが対応づけられている。尚、公開鍵データは、予めそれぞれの宛先からLAN経由で取得するか、若しくは、通信装置201に着脱可能な記憶媒体をドライブする装置を接続する機能を具備させて、該記憶媒体を介して取得する。取得した公開鍵データはファイルデータとして格納しておき、所定操作によりアドレス帳に取得した公開鍵と宛先と対応づけておく。

【0037】また、公開鍵を取得する際に、所定の認証機関により当該公開鍵が本人のものであることを証明する証明書を合わせて受け取り、該公開鍵の正当性を確認した後、公開鍵を上記アドレス帳に登録する手順をとると好適である。

【0038】では、図6および図7を用いて、本実施形態を説明する。

【0039】まず、公衆回線網202からサブアドレス「0123」が指定された画像データを受信すると、図6の管理テーブルから転送先の電子メールアドレスは「aaa@xxx.xxx.com」と変換され、さらに図7のアドレス帳から転送先の電子メールアドレスをキーとして公開鍵の有無が判別される。

【0040】したがって、図6および図7の例によれば、サブアドレス「0123」および「8901」が指定された親展画像については、公開鍵を所有していないので、それぞれ、対応するメモリボックス「01」および「03」に格納され、格納した親展ボックス番号や、送信元情報、受信日時をテキストデータとして記載した電子メールをそれぞれの転送先である「aaa@xxx.xxx.com」および「ccc@xxx.xxx.com」に転送する。

【0041】サブアドレス「4567」が指定された親展画像については、公開鍵を所有しているので、その公開鍵により親展画像を暗号化して、転送先である「bb@xxx.xxx.com」に転送する。

【0042】また、受信した画像データが親展画像でない場合には、サブアドレスに対応した転送先の電子メールアドレスに対して、受信した画像データを暗号化せずに電子メールで転送する。

【0043】図5は、本実施形態における通信装置201の動作を示すフローチャートである。ここでステップS501～505の処理については、上記第1の実施形態のステップS301～305において説明しているので、ステップS506から説明する。

【0044】まずステップS506において、ステップS504で受信した画像データが親展画像であるか否かを判別し、親展画像でない場合にはステップS512に進み、ステップS503で受信したサブアドレスに対応する転送先の電子メールアドレスに該受信した画像データを添付した電子メールを送信する。

【0045】ステップS507では、ステップS503で受信したサブアドレスに対応する電子メールアドレスに公開鍵が関連づけられているか否かを上記図6の管理テーブルおよび図7のアドレス帳に基づいて判断する。公開鍵が関連づけられていない場合には、ステップS510に進み、受信した画像データをサブアドレスに対応するメモリボックスに格納する。そしてステップS511で、サブアドレスに対応する電子メールアドレスに対して、親展画像をメモリボックスに格納した旨のメッセージを本文データとして記載した電子メールを送信する。該メッセージの例として、「あなたのメモリボックスに親展画像を受信しましたので受け取りに来てください」等を用いればよい。

【0046】ここで、該メッセージを記載した電子メールを受信した親展画像の受取人が、通信装置201の設置場所まで出向き、上記メモリボックスに対応するパスワードを操作パネル105から入力することにより、親展画像が不図示のプリンタから出力される。これにより、親展画像が暗号化されないまま不用意にLAN上に送出されることがなくなり親展画像の機密性を維持することが可能となる。

【0047】ステップS507の判断で、公開鍵が関連づけられている場合には、ステップS508に進み、受信した画像データを該公開鍵で暗号化し、ステップS509で該暗号化した親展画像を添付した電子メールにより転送する。公開鍵による暗号化方式としては、例えばRSA (Rivest-Shamir-Adleman) 方式等がある。

【0048】以上の処理により、公衆回線網から受信した親展画像をLAN経由で転送する際に、確実に暗号化して転送することが可能となり、親展画像の機密性が維持される。

【0049】尚、暗号方式には上記の公開鍵方式の他に共通鍵方式がある。共通鍵方式は、送信側の暗号化鍵と受信側の復号化鍵とが同じ暗号鍵であり、その暗号鍵によって送信側で通信文(平文)を暗号化して送信し、受信側で受け取った通信文(暗号文)を同じ暗号鍵で復号化するものである。

【0050】一般に公開鍵方式は、共通鍵方式にくらべて、暗号化とその解読の処理が複雑で時間がかかる傾向があるので、所定のアルゴリズムにより生成した共通鍵により親展画像を暗号化したデータと、該共通鍵を転送先の公開鍵で暗号化したデータとを転送するようにしてもよい。共通鍵による暗号化方式としてはDES (Data Encryption Standard) 方式等がある。

【0051】<第4の実施形態>上記第3の実施形態では、上記ステップS510において、メモリボックスに格納した親展画像の受取人は、通信装置201に出向いてプリント出力するものとして説明したが、本実施形態では、親展画像をメモリボックスに格納した後、該親展画像の転送先の公開鍵が上記アドレス帳に登録されたことを契機として、自動的に該親展画像を該公開鍵で暗号化して転送先に転送するものである。

【0052】これにより、親展画像の受取人がわざわざ通信装置201まで出向かなくても、管理者等に公開鍵を登録してもらうか、LAN203経由で公開鍵を通信装置201に送れば、メモリボックス内の親展画像を取得することが可能となる。

【0053】本実施形態における通信装置201の動作を図9のフローチャートを参照して説明する。尚、図9のフローチャートは第3実施形態のフローチャートをモディファイしたものであり、同一符号のステップについては、同一の処理であることを示している。以下、処理の異なるステップについて説明する。

【0054】まず、図10のステップS511の処理後、メモリボックスに格納した親展画像に対応する宛先の公開鍵がアドレス帳に登録されたか否かを判定する判定プロセスを所定周期で実行し(ステップS1001、ステップS1002のループ処理)、ステップS1001において、該判定プロセスの肯定判定を検出したら、ステップS508に進み、登録された公開鍵により親展画像を暗号化して転送を行う。

【0055】また、ステップS511で送信するメッセージとして、「あなたのメモリボックスに親展画像を受信しましたので、あなたの公開鍵をお送りいただければ暗号化して送信します。」等を用いればよい。

【0056】<第5の実施形態>上記第3の実施形態では、転送先の公開鍵を保持していない場合には一律に転送を実行しないようにしたが、本実施形態は、転送経路のセキュリティに応じて暗号化転送を実行するものである。すなわち、LAN203経由の転送において、転送経路のセキュリティが確保されていない場合に限り、

転送先の公開鍵の有無を判断し、該判断の結果、公開鍵が有れば親展画像を暗号化して転送し、公開鍵が無ければ親展画像をメモリボックスに格納してその旨のメッセージのみを転送先に送信する。また、転送経路のセキュリティが確保されている場合には、転送先の公開鍵の有無にかかわらず、親展画像を転送先に転送する。

【0057】これにより、イントラネット等のセキュリティが確保されているドメイン内の転送先に対しては、公開鍵データのやりとりが不要となり、通信装置201の登録データを管理する手間を軽減することができる。

【0058】本実施形態における通信装置201の動作を図10のフローチャートを参照して説明する。尚、図10のフローチャートは上記第3実施形態の図5のフローチャート図をモディファイしたものであり、同一符号のステップについては、同一の処理であることを示している。以下、処理の異なるステップについて説明する。

【0059】まず、ステップS506において受信した画像データが親展画像であると判断されるとステップS1101に進む。ステップS1101ではステップS503で受信したサブアドレスに対応した転送先の転送経路のセキュリティを判断し、転送経路にセキュリティ有り

と判断した場合には、ステップS512に進み親展画像を該転送先に転送する。

【0060】また、転送経路にセキュリティ無しと判断した場合にはステップS507に進み、公開鍵の有無に基づいて親展画像を転送するかメモリボックスに格納するかを決定する。ここでステップS1101における転送経路のセキュリティの有無の判断は、例えば通信装置210の電子メールアドレスのドメインと転送先の電子メールアドレスのドメインに基づいて判断すればよい。

【0061】その判断を、図6および図7を参照して説明する。前に述べたように通信装置201の電子メールクライアント機能を備えており、その電子メールアドレスを「fax@xxx.xxx.com」とする。

【0062】したがって、図7のアドレス帳データの例によれば、宛先aaa、bbb、及び、cccが通信装置201と同一ドメイン「xxx.xxx.com」内にあり、宛先ddd、及び、eeeが通信装置201とは異なるドメインにあることがわかる。

【0063】そこで、通信装置201と同一のドメイン内の転送先については、アドレス帳に公開鍵が登録されているか否かにかかわらず、親展画像を添付した電子メールにより転送を行う。

【0064】通信装置201と異なるドメイン内の転送先については、アドレス帳に公開鍵が登録されているか否かに応じた方式により転送を行う。すなわち、宛先dddは公開鍵が登録されていないので、ddd宛ての親展画像は対応するメモリボックス04に格納し、宛先dddに対してはメモリボックス04に親展画像を格納したメッセージを本文に記載した電子メールのみを送信す

る。また、宛先eeeに対しては、公開鍵が登録されているので、該公開鍵により暗号化した親展画像を添付した電子メールをeee宛てに送信する。

【0065】尚、ドメイン名はドット(dot)で区切った階層構造になっており、第1階層である「com」を起点としてどの層までの一致をもって同一ドメインと判断するかは、ネットワークシステムのセキュリティポリシーに基づくので、例えば、「xxx.com」の第2階層までの一致をもって転送経路のセキュリティ有り

と判断してもよい。

【0066】また、上記の例はドメイン名に基づいた判断であるが、転送先のIPアドレスのサブネットが所定のサブネットの範囲内にあるか否かに基づいてセキュリティの有無を判断してもよい。

【0067】＜第6の実施形態＞公開鍵には、機密性を高めるために期限付きで有効になるものがある。本実施形態では、このような公開鍵を利用する場合について図11を参照して説明する。

【0068】尚、図11のフローチャートは上記第3実施形態の図5のフローチャート図をモディファイしたものであり、同一符号のステップについては、同一の処理であることを示している。以下、処理の異なるステップについて説明する。

【0069】まず、ステップS506において受信した画像データが親展画像であると判断されると、ステップS507において、ステップS503で受信したサブアドレスに対応する電子メールアドレスに公開鍵が関連づけられているか否かを上記図6の管理テーブルおよび図7のアドレス帳に基づいて判断する。

【0070】ステップS507で公開鍵が関連づけられていると判断された場合は、ステップS1201において、その公開鍵が有効期限内かどうか判定する。

【0071】ステップS1201で公開鍵が有効期限内であれば、ステップS508において、受信した画像データを該公開鍵で暗号化する。そして、ステップS509において、該暗号化した親展画像を添付した電子メールにより転送する。

【0072】ステップS1201において、公開鍵が有効期限切れであれば、ステップS510において、受信した画像データをサブアドレスに対応するメモリボックスに格納する。そして、ステップS511において、サブアドレスに対応する電子メールアドレスに対して、親展画像をメモリボックスに格納した旨のメッセージを本文データとして記載した電子メールを送信する。該メッセージの例として、「公開鍵の有効期限が切れていいます。あなたのメモリボックスに親展画像を受信しましたので受け取りに来てください」等を用いればよい。

【0073】また、公開鍵の有効期限が更新されたことを契機として、自動的に該親展画像を該公開鍵で暗号化して転送先に転送するようにしてもよい。

【0074】この場合の通信装置 201 の動作を図 12 のフローチャートを参照して説明する。尚、図 12 のフローチャートは第 3 実施形態のフローチャートをモディファイしたものであり、同一符号のステップについては、同一の処理であることを示している。以下、処理の異なるステップについて説明する。

【0075】まず、図 12 のステップ S511 の処理後、ステップ S1304 において、メモリボックスに格納した親展画像に対応する宛先の公開鍵の有効期限が更新されたか否かを判定する判定プロセスを所定周期で実行し（ステップ S1302、ステップ S1303 のループ処理）、ステップ S1302 において、該判定プロセスの肯定判定を検出したら、ステップ S1301 に進み、更新された期限が有効か否かを判定する。

【0076】ステップ S1301 で公開鍵が有効期限内であると判定されれば、ステップ S508 において、受信した画像データを該公開鍵で暗号化する。そして、ステップ S509 において、該暗号化した親展画像を添付した電子メールにより転送する。

【0077】また、ステップ S511 で送信するメッセージとして、「公開鍵の有効期限が切れています。あなたのメモリボックスに親展画像を受信しましたので、あなたの公開鍵の有効期限更新手続きをしていただければ暗号化して送信します。」等を用いればよい。

【0078】尚、本実施の形態では、公開鍵の有効期限を更新する場合について述べたが、転送先から新たに有効期限内にある公開鍵を取得したことを契機として、所定のメモリボックスに格納された親展画像を暗号化して転送するようにしても良い。

【0079】＜第 7 の実施形態＞上記実施形態では、通信装置という 1 つの機器を用いた動作により説明したが、パーソナルコンピュータ及びモデム、スキャナ、プリンタ等の複数の機器から構成されるシステムに本発明を適用してもよい。図 8 を用いてそのシステム構成を簡単に説明する。同図より、パーソナルコンピュータ 802（以下、PC802 と称する）に、スキャナ 801、プリンタ 803、モデム 804（PC802 に内蔵されている）が、所定のインターフェースを介して接続されている。また、PC802 は、モデム 804 を介して公衆回線網 202 に接続され、不図示の LAN ボードを介して LAN203 に接続されている。

【0080】尚、PC802 と、スキャナ 801、および、プリンタ 803、および、モデム 804 との接続インターフェースは、LAN203 を介したネットワークインターフェースであってもよいが、親展画像等の秘匿データを扱う関係上、USB 等の LAN203 と分離されたローカルインターフェースが好適である。

【0081】このシステムでの受信動作について説明すると、まず、公衆回線網 202 から送られてきた信号はモデム 805 に内蔵された NCU 部を介してモデム 80

5 へ取り込まれる。モデム 805 ではこのアナログ信号を復調して、デジタルデータを復元する。このデジタルデータはコンピュータ 807 から読み出され、圧縮データの解凍により画像データを復元したのち、プリンタ 808 へ送られる。プリンタ 808 ではこの画像データを印刷する。

【0082】このとき受信した画像データが親展であれば、PC802 が内蔵するハードディスク装置内のメモリボックスに格納され、上記第 3 実施形態によれば、公開鍵データを有する宛先に対しては該公開鍵により暗号化して親展画像を転送し、公開鍵データを有しない宛先に対しては親展画像を受信した旨を記述した電子メールを送信する。

【0083】以上、第 1 ～ 7 の実施形態について説明したが、これらの実施形態では、送信機から受信したサブアドレスを本発明に係る通信装置が電子メールアドレスに変換する例を示したが、送信機からのサブアドレス内に転送先の電子メールアドレスが直接セットされている形態であってもよい。

【0084】また、上記実施形態では、公衆回線網 202 からの受信した画像データを LAN203 上のクライアント装置に宛てに転送する例を用いて説明したが、これに限定されるものではなく、LAN203 が所定のアクセスポイントを介してインターネットに接続された構成において、公衆回線網 202 からの受信した画像データをインターネット経由で転送してもよい。インターネットを経由した通信についてはそのセキュリティが重要視されており、本発明は好適である。

【0085】尚、公衆回線網からの受信した画像データを、該公衆回線網からインターネットのアクセスポイントへダイアルアップ接続して転送する場合にも、本発明は適用される。

【0086】また、本発明はシステム或は装置にプログラムを供給することによって達成される場合にも適用できることは言うまでもない。その場合、記憶媒体に格納された本発明を達成するためプログラムコードを該システム或は装置のコンピュータ（CPU もしくは MPU）が読み出し実行することによって、本発明の目的が達成される。

【0087】また、本発明は、コンピュータが読み出したプログラムコードを実行する際に、コンピュータ上で稼動している OS（オペレーティングシステム）などが処理の一部を行うような場合も含むことは言うまでもない。

【0088】

【発明の効果】以上説明したように、本出願の発明によれば、公衆回線網から受信した親展画像を暗号化して LAN 上のサーバコンピュータに保存することにより、特定のクライアント以外のユーザが、容易に親展画像を閲覧できないようになり、機密性を維持したまま親展画像

をLAN上のクライアントに配信することが可能となる。

【0089】また、本出願の発明によれば、受信した親展画像を電子メールに添付して該画像の受取人であるユーザへ送信するようにしたので、該ユーザは、通信装置までわざわざ出向いて親展画像を印刷するような手間が無くなり、ユーザの操作負荷が著しく軽減される。

【0090】また、本出願の発明によれば、転送先の暗号鍵を保持している場合には、該暗号鍵により暗号化して転送し、保持していない場合には、所定のメモリボックスに格納するようにしたので、親展画像が暗号化されずに、不用意にLAN上に流出してしまうのを防止することができる。

【0091】また、本出願の発明によれば、親展画像をメモリボックスに格納した後、該親展画像の転送先の暗号鍵が登録されたことを検出したら自動的に該親展画像を該公開鍵で暗号化して転送先に転送するようにしたので、ユーザが親展画像を受け取るためわざわざ装置まで出向く必要がなくなる。

【0092】また、本出願の発明によれば、転送経路のセキュリティに基づいて暗号化転送を実行するようにしたので、セキュリティの確保されたネットワーク内での転送に際しては、暗号鍵のやりとりの手間がなくなり、装置管理者の負荷を軽減することが可能となる。

【0093】また、本出願の発明によれば、転送先の暗号鍵が有効期限内であれば、該暗号鍵により暗号化して転送するようにしたので、信頼性の高い暗号鍵により暗号化された親展画像を転送することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態における通信装置の構成を示した図

【図2】本発明の第1実施形態におけるネットワークシステムを示した図

【図3】本発明の第1実施形態における通信装置の動作を示すフローチャート

【図4】本発明の第2実施形態における通信装置の動作を示すフローチャート

【図5】本発明の第3実施形態における通信装置の動作を示すフローチャート

【図6】本発明の第3実施形態におけるサブアドレスと電子メールアドレスの対応を示した管理テーブルのデータ構造を示した図

【図7】本発明の第3実施形態におけるアドレス帳のデータ構造を示した図

【図8】本発明の第7実施形態における通信装置システムの構成を示した図

【図9】本発明の第4実施形態における通信装置の動作を示すフローチャート

【図10】本発明の第5実施形態における通信装置の動作を示すフローチャート

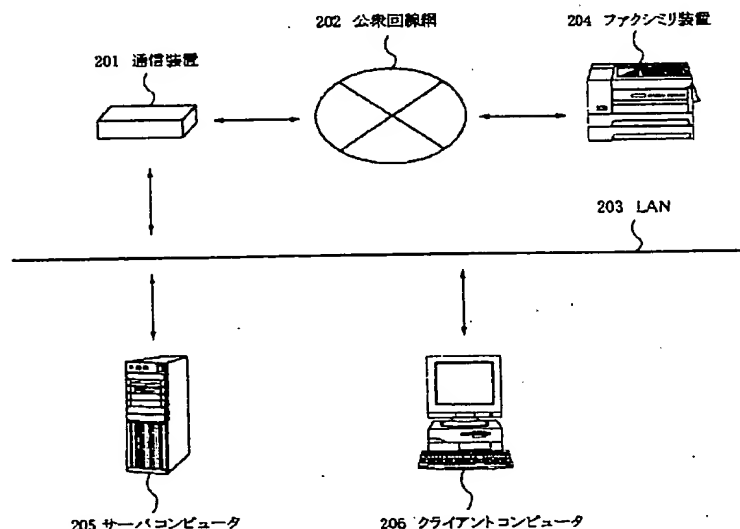
【図11】本発明の第6実施形態における通信装置の動作を示すフローチャート

【図12】本発明の第6実施形態における通信装置の動作を示すフローチャート

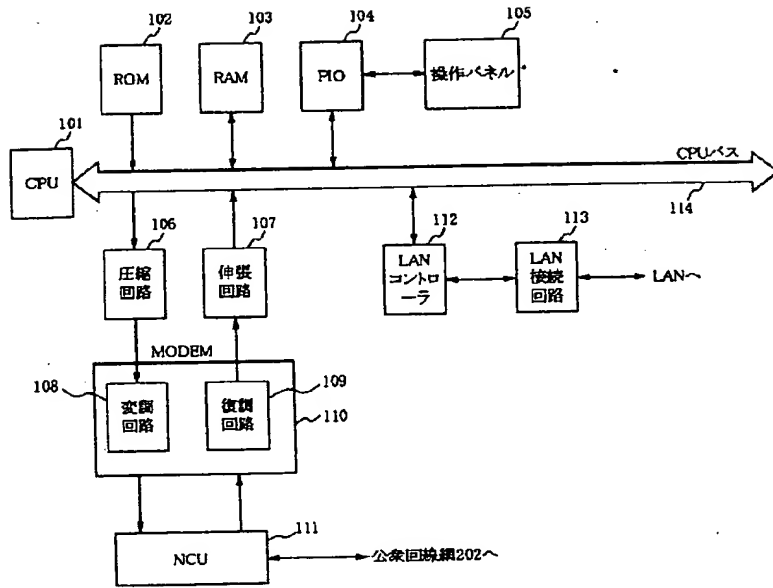
【符号の説明】

- 201 通信装置
- 202 公衆回線網
- 203 LAN
- 204 ファクシミリ装置
- 205 サーバコンピュータ
- 206 クライアントコンピュータ

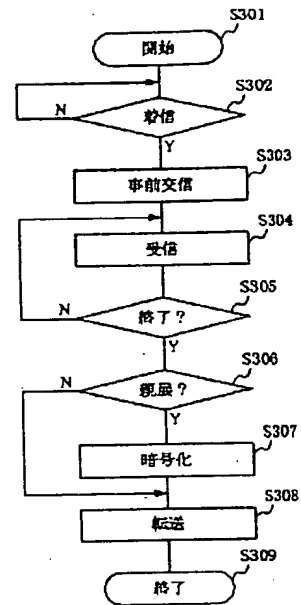
【図2】



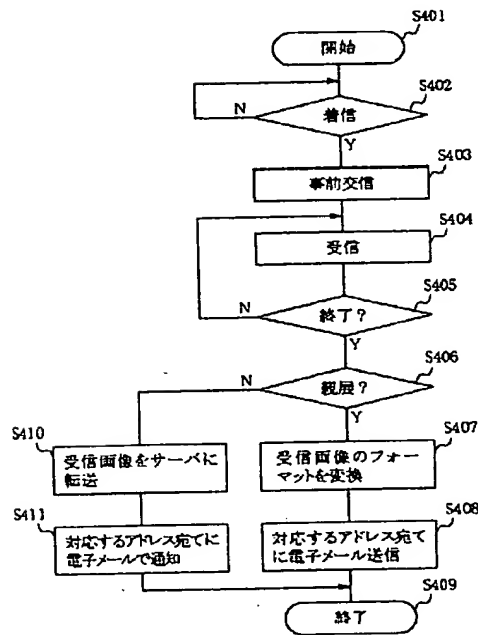
【図 1】



【図 3】



【図 4】



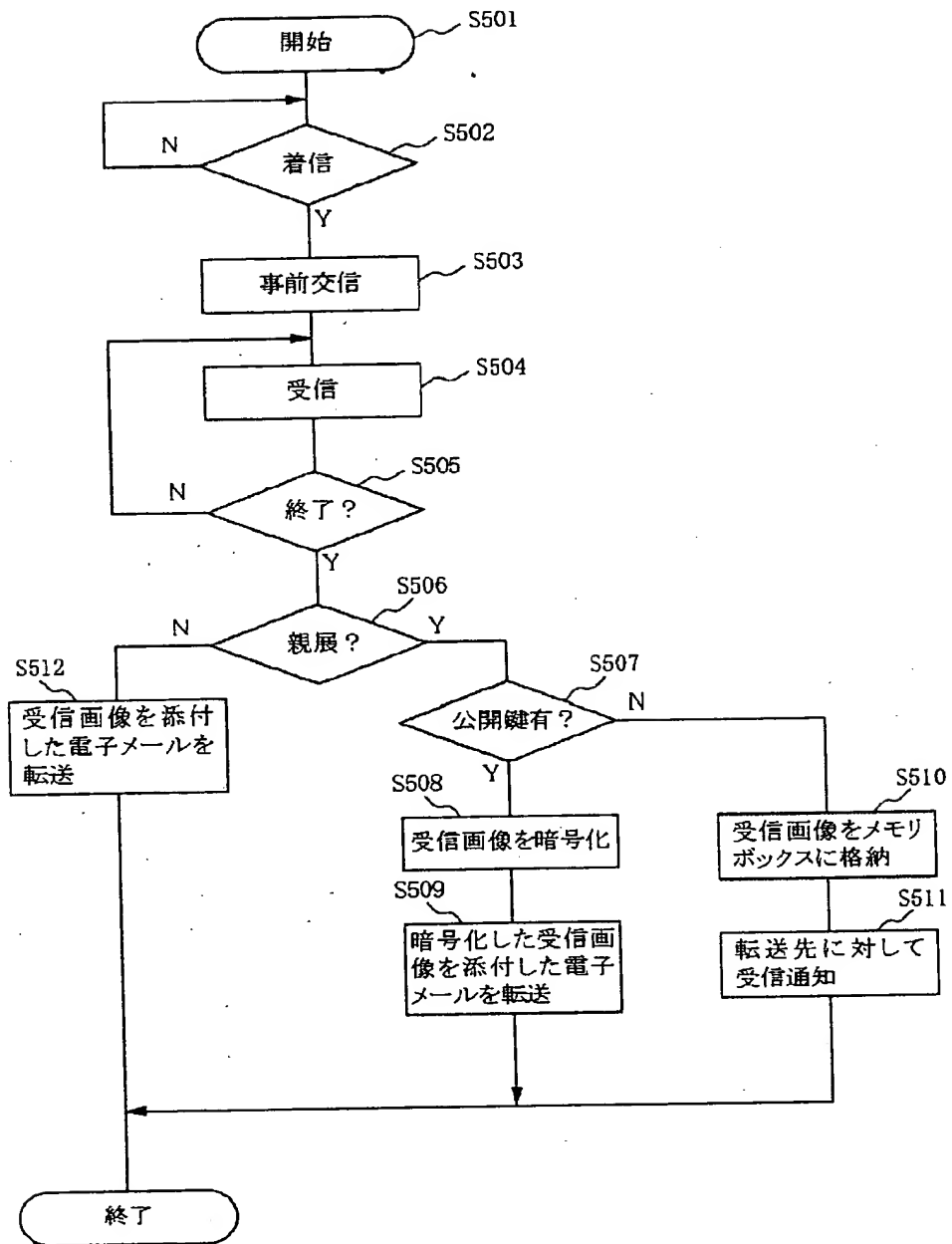
【図 6】

| サブアドレス | 転送先の電子メールアドレス | メモリボックス |
|--------|------------------------|---------|
| 0123 | aaa@canon. canon. com | 01 |
| 4567 | bbb@canon. canon. com | 02 |
| 8901 | ccc@canon. canon. com | 03 |
| 2345 | ddd@canon2. canon. com | 04 |
| 6789 | eee@canon2. canon. com | 05 |

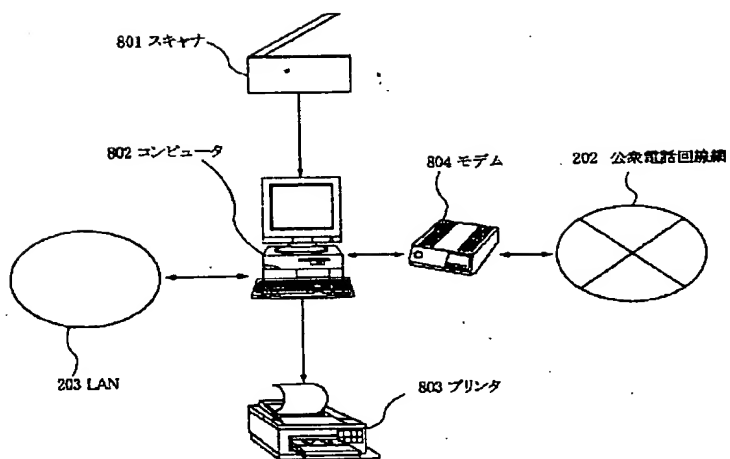
【図 7】

| 宛先名 | 電子メールアドレス | 公開鍵 |
|-----|------------------------|--------|
| aaa | aaa@canon. canon. com | 無し |
| bbb | bbb@canon. canon. com | 公開鍵bbb |
| ccc | ccc@canon. canon. com | 無し |
| ddd | ddd@canon2. canon. com | 無し |
| eee | eee@canon2. canon. com | 公開鍵eee |

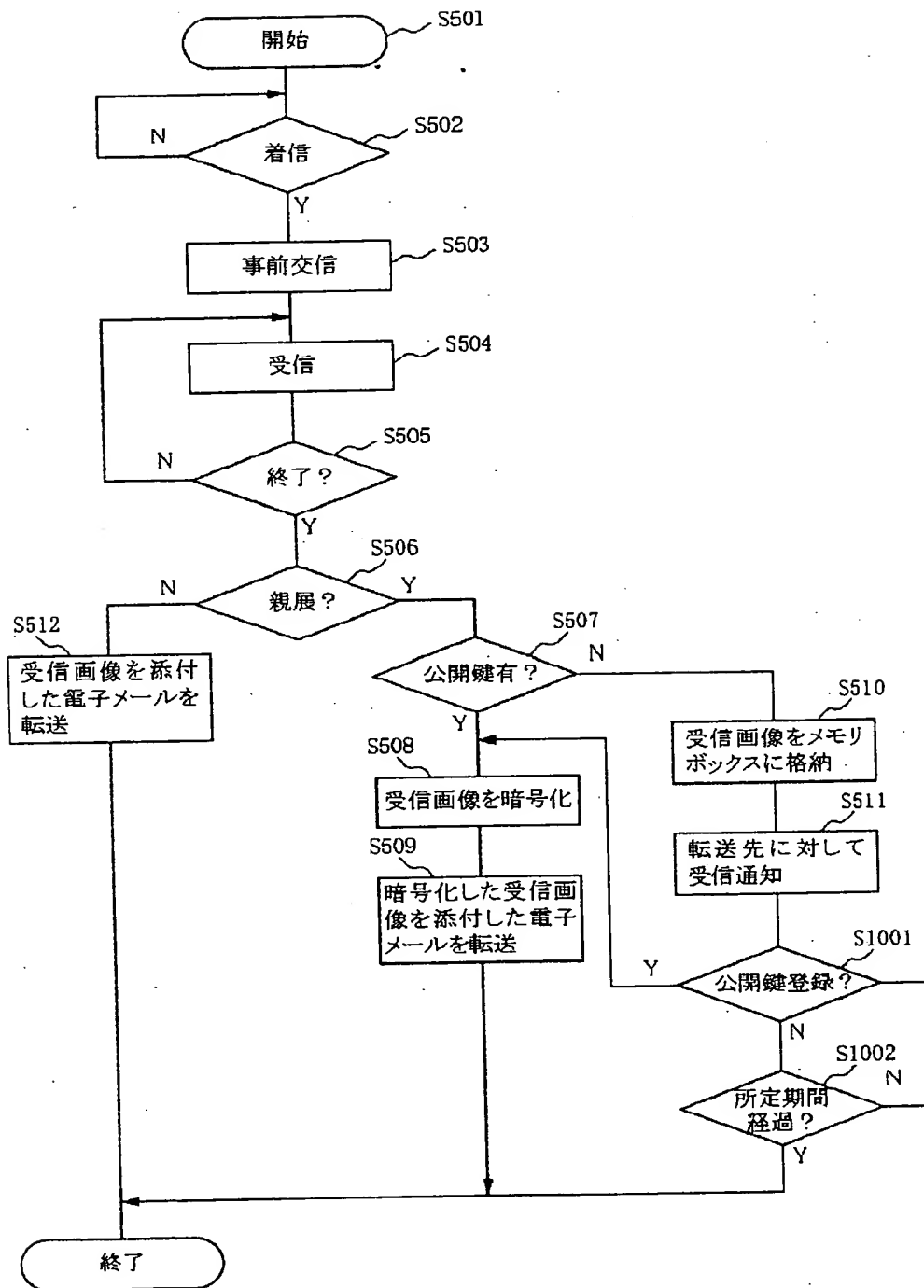
【図 5】



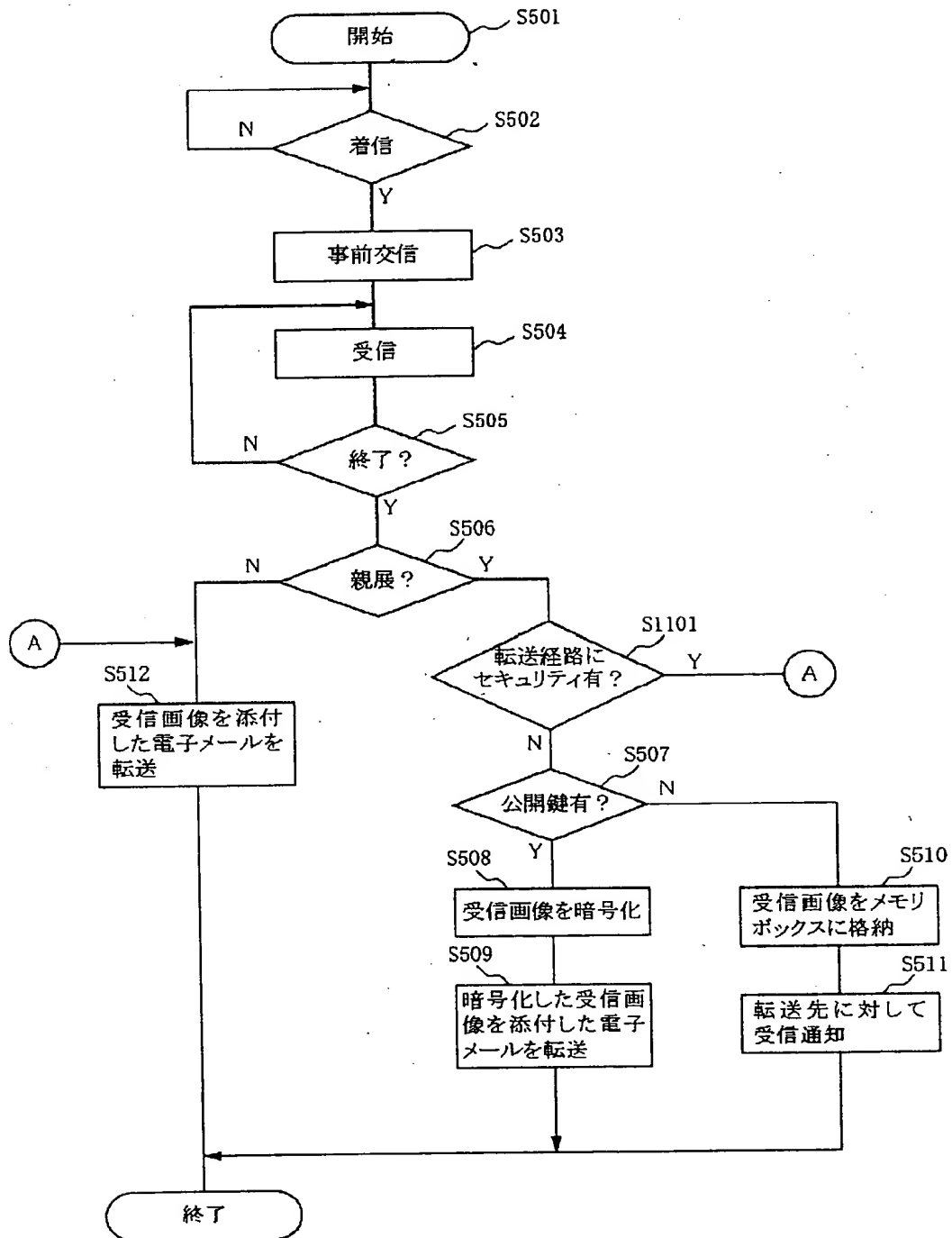
【図 8】



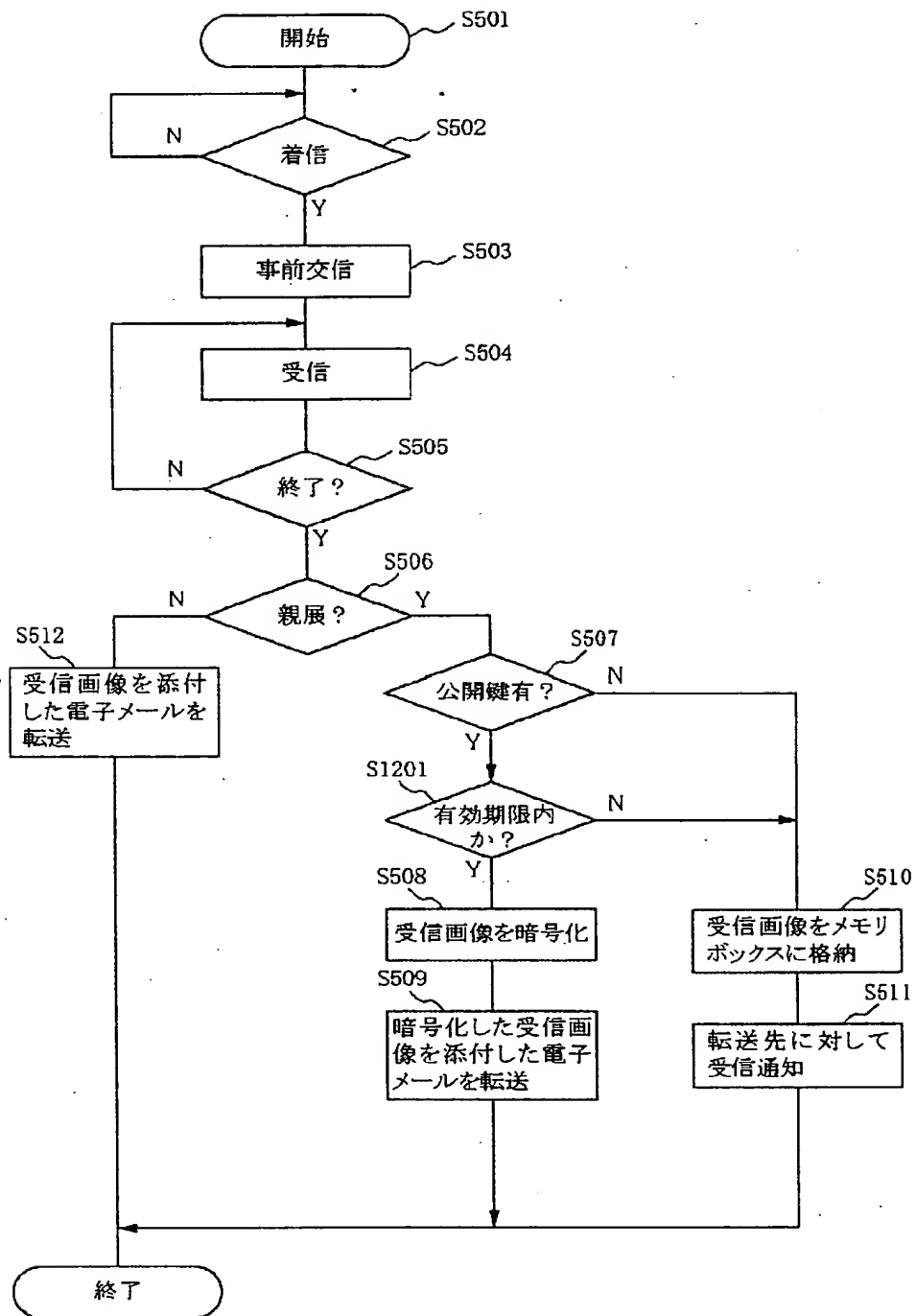
【図 9】



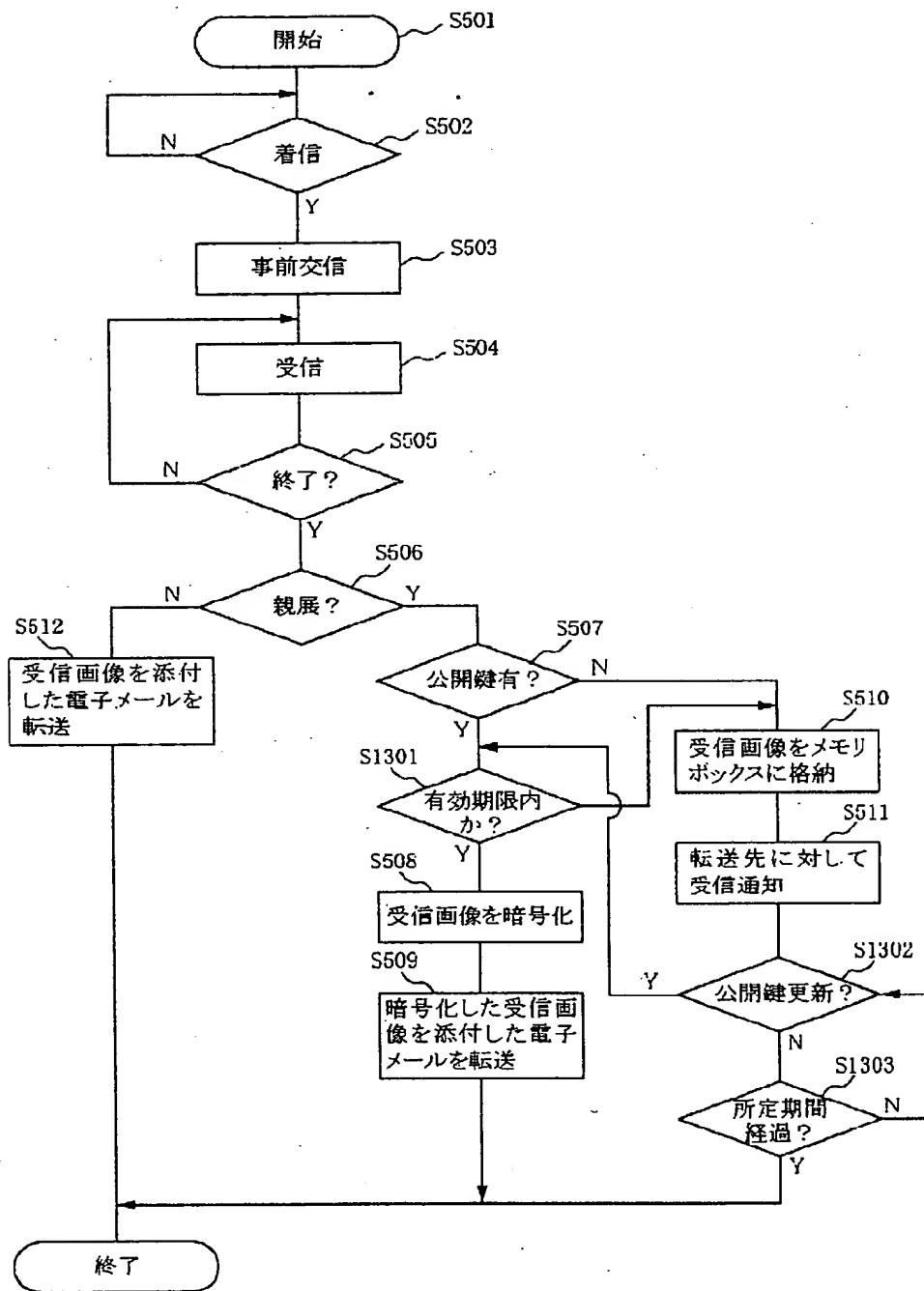
【図 10】



【図 11】



【図 12】



フロントページの続き

(51) Int. Cl.⁷H04N 1/00
1/44

識別記号

104

FI

H04L 11/20

テ-マコード (参考)

B